

AFRL-IF-RS-TM-2006-2
Technical Memorandum
March 2006



AIR FORCE ENTERPRISE DEFENSE (AFED)

Northrop Grumman

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TM-2006-2 has been reviewed and is approved for publication.

APPROVED: /s/

BRIAN T. SPINK
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE MARCH 2006	3. REPORT TYPE AND DATES COVERED Tech Memo Apr 03 – Aug 04		
4. TITLE AND SUBTITLE AIR FORCE ENTERPRISE DEFENSE (AFED)		5. FUNDING NUMBERS C - F30602-99-D-0001/0020 PE - 33140F PR - 7820 TA - JM WU - 20		
6. AUTHOR(S) Lou Scheiderich				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Northrop Grumman 7575 Colshire Drive McLean Virginia 22102		8. PERFORMING ORGANIZATION REPORT NUMBER N/A		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/IFGA 525 Brooks Road Rome New York 13441-4505		10. SPONSORING / MONITORING AGENCY REPORT NUMBER AFRL-IF-RS-TM-2006-2		
11. SUPPLEMENTARY NOTES AFRL Project Engineer: Brian T. Spink/IFGA/(315) 330-7596/ Brian.Spink@rl.af.mil				
12a. DISTRIBUTION / AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 Words) Provided technical Information Assurance (IA) support to the Air Force Research Laboratory (AFRL) Defensive Information Warfare (DIW) Branch in the design, development, integration, installation and demonstration of the Air Force Enterprise Defense (AFED) and Automated Intrusion Detection Environment (AIDE) systems.				
14. SUBJECT TERMS Sort Finder, Drilldown			15. NUMBER OF PAGES 15	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	

TABLE OF CONTENTS

1.0 What is AFED?	1
2.0 Background:	1
3.0 Before AFED	1
4.0 AIDE (Automated Intrusion Detection System)	2
5.0 EPIC (Extensible Prototype for Intrusion Command and Control)	2
6.0 AFED Database	2
7.0 DATA Extraction Utility	3
8.0 SQL Correlator	3
9.0 FlexViewer	4
10.0 AIDE (Automated Intrusion Detection System)	4

LIST OF FIGURES

Figure 1: AFED Conceptual Architecture	5
Figure 2: AFED Components	6
Figure 3: AFED FlexViewer	6
Figure 4: FlexViewer – Editor Window	7
Figure 5: FlexViewer – Sort Finder	7
Figure 6: FlexView – Color Code Editor	8
Figure 7: FlexViewer – Color Codes Applied	8
Figure 8: Hose POC - Drilldown	9
Figure 9: Hose Services - Drilldown	9
Figure 10: Data View	10
Figure 11: Data View – Tuning Applied	10
Figure 12: Data View – Organization Drilldown	11

1.0 What is AFED?

AFED is a security management system combining data from multiple types of sensors including IDS, vulnerability assessment, change management, correlators, etc.

1.1 Allows analyst to view data from a single console.

1.2 Aggregation capabilities significantly reduce data that must be viewed by analysts.

1.3 AFED components are configurable and flexible to allow them to be quickly modified to accept, aggregate and display information from new data sources.

2.0 Background:

2.1 Development – 2000 to 2004

2.2 Built on EPIC, AIDE, EPIC2 systems

2.3 Started as AC2ISRC funded program, then supported by In-House funding

Initiated to address Warfighter needs for better network security tools

2.4 Installations at ACC NOSC (2000), AFIWC (2002) and AFRL/RRS NOC 2002

2.5 Core system completed Jan 2004

3.0 Before AFED:

3.1 EPIC (Extensible Prototype for Intrusion Control)

- 1997-1998
- Designed to collect information from Multiple Data Sources
- Based upon G2 Expert System
- Demonstrated at EFX 98, JBC 98

4.0 AIDE (Automated Intrusion Detection System)

4.1 1998 to 2002

4.2 DISA ATD built on EPIC focused on Intrusion Detection and Hierarchical Reporting.

4.2.1 Deployed to 15+ DISA sites

5.0 EPIC (Extensible Prototype for Intrusion Command and Control)

- 1999 to 2000
- Enhanced version of EPIC
- New features included
 - additional database support
 - Policy enforcement capability
 - Host information
 - Network Management

6.0 AFED Database

6.1 Application – Oracle 9i Database

6.2 Types of Data Stored

- Host/Network based intrusion detection events (including syslog events)
 - . OS
 - . Location
 - . Services/service approval status
 - . POC data
 - . Vulnerability data
 - . Mission data
- Signature References, Analyst defined Notes/COA's
- Signature Normalization data
- IP domain to Organization mappings and metadata

7.0 DATA Extraction Utility

7.1 Application – Java based client/server

7.2 Capabilities

- Robust communication of data from files/databases to another database
- Supports Oracle, MySQL, Postgres, and Access
- Extreme configurability (configuration file specifies parsing, filtering, connections, etc.)
- Bookmarking
 - . Tracks what data was read and transferred
 - . Prevents loss of data in the event of a shutdown or network failure
 - . Source quenching
 - . Throttling mechanism that buffers data at server side to prevent overrun of database
- Health status reporting
- Can be used independently of AFED database and FlexViewer

8.0 SQL Correlator

8.1 Application

- Java based application based on FlexViewer
- Writes results to database

8.2. Capabilities

- Generate new “Cyber Alerts” regarding conditions that can be determined from SQL queries and insert them into database.
 - Extreme configurability
 - Read/write to any database schema
 - Supports Oracle, MySQL, Postgres, and Access
 - Can be used independently of AFED database and Data Extraction Utility and FlexViewer

9.0 *FlexViewer*

9.1 Application

- Java Based Graphical User Interface
- Provides a spreadsheet view of data
- Graphical capability to be added

9.2 Capabilities:

- Displays Data from Oracle, MySQL, Postgres, and Access
- Drive third party apps using data from spreadsheet cells
- Fully configurable menus
- User definable/sharable
- Built-in scripting engine allowing extreme extensibility
- Can be used independently of AFED database and Data Extraction Utility

10.0 *AIDE (Automated Intrusion Detection System)*

10.1 1999 TO 2000

10.2 Enhanced version of EPIC

10.3 New features included:

10.1.1 Additional database support

10.1.2 Policy enforcement capability

10.1.3 Host information

10.1.4 Network Management

AFED Conceptual Architecture

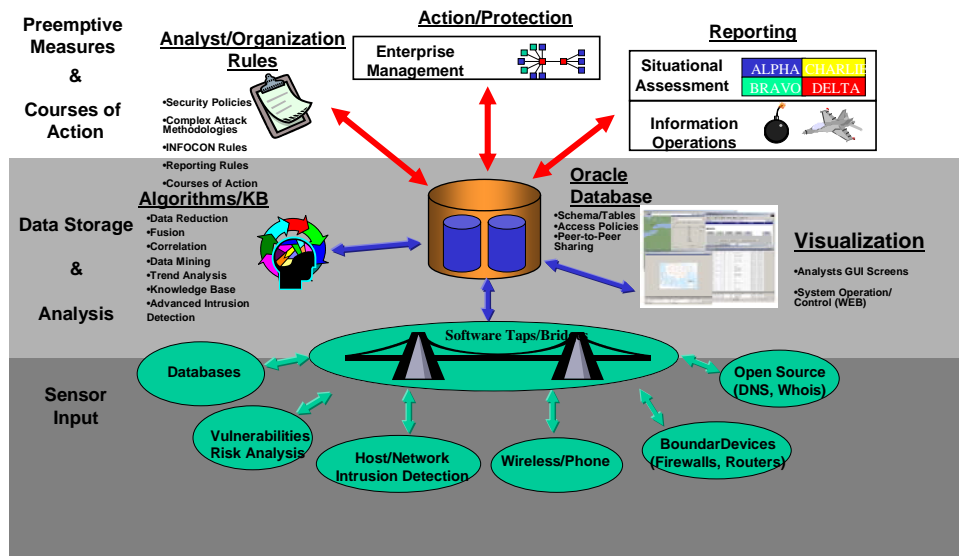


Figure 1: AFED Conceptual Architecture

AFED Components

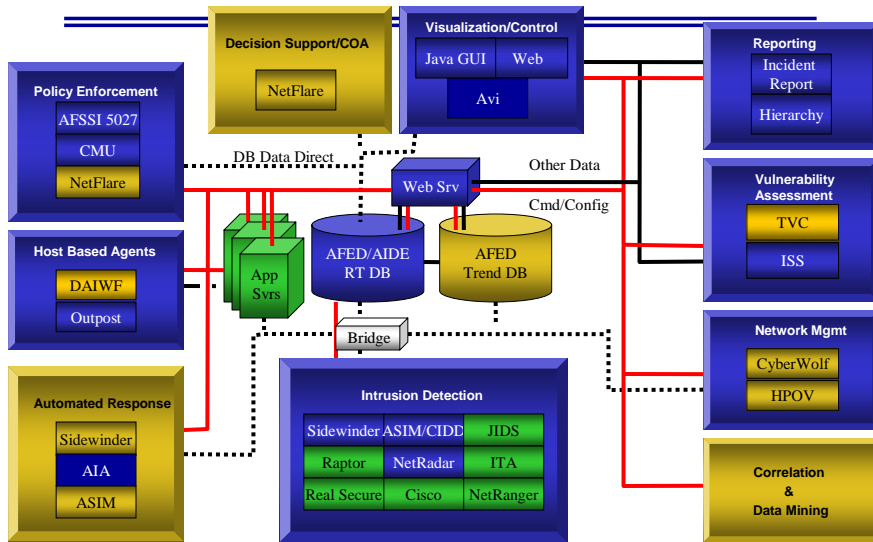


Figure 2: AFED Components

AFED FlexViewer

[illegible]

Figure 3: AFED FlexViewer

FlexViewer - Editor Window

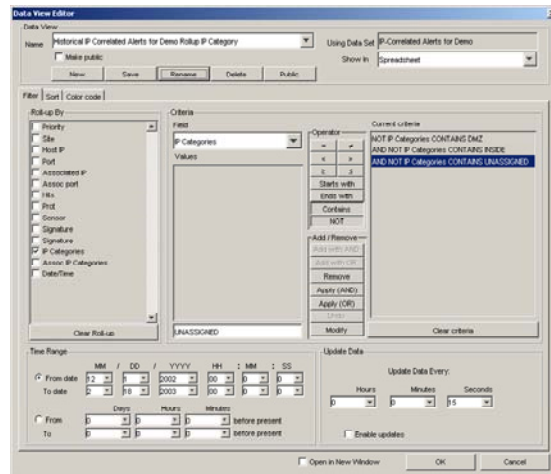


Figure 4: FlexViewer – Editor Window

FlexViewer - Sort Editor

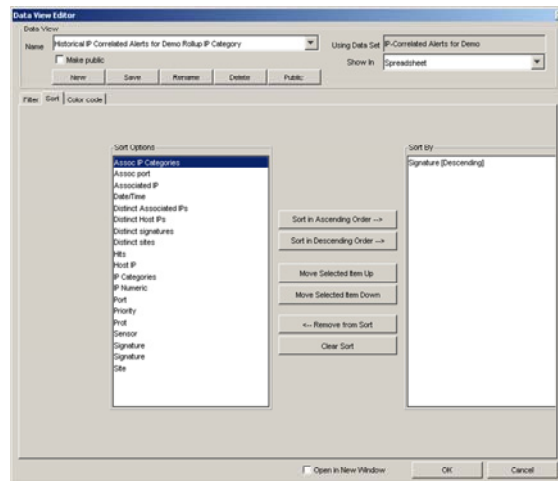


Figure 5: FlexViewer – Sort Finder

FlexViewer - Color Code Editor

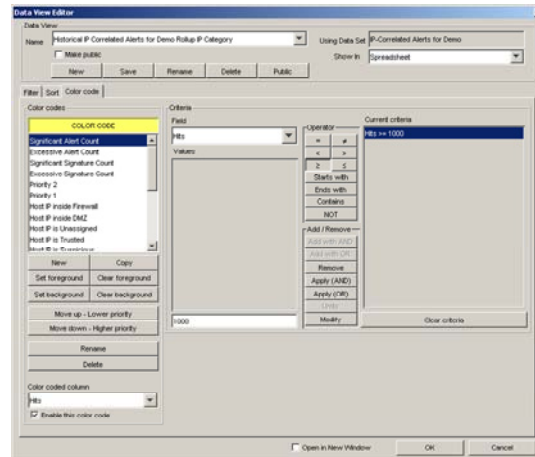


Figure 6: FlexView – Color Code Editor

FlexViewer - Color Codes Applied

The screenshot shows the FlexViewer interface with a table of alerts. The table has columns for 'Alert ID', 'Alert Name', 'Alert Category', 'Alert Status', 'Alert Time', 'Alert Source', 'Alert Destination', 'Alert Action', and 'Alert Comment'. The rows are color-coded based on the 'Alert Category' column. The table is titled '1119 LOGS 1679 ZONE'. The status bar at the bottom shows 'INFOCON: NORMAL' and 'REPORT STATUS'.

Figure 7: FlexViewer – Color Codes Applied

Host POC Drilldown

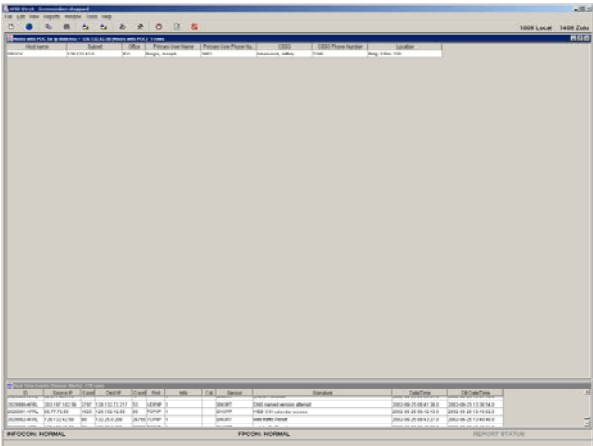


Figure 8: Hose POC - Drilldown

Host Services Drilldown

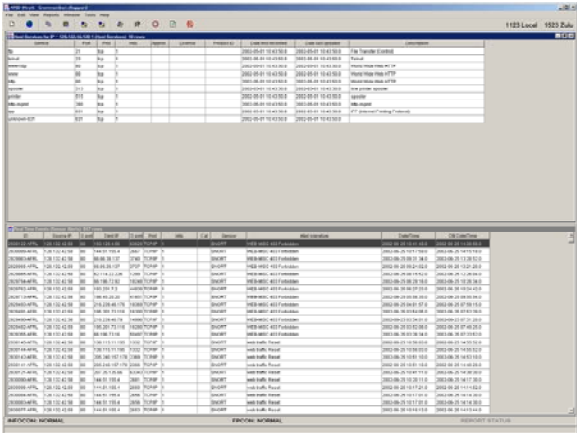


Figure 9: Hose Services - Drilldown

Data View

Sorted by Hits

FullDataset Bullog sig (Sensor Alerts) 474 rows from 77567 records										
Site	Source IP	Port	Dest IP	Port	Hits	Prot	Signature	Source IP Cat	Source Org	
3*	31*	-1	6498*	-1	171,451	OMP	OMP PING Sun Solars	3*	23*	
3*	4576*	15909*	222*	80	49,641	TCP	WEBFRONTPAGE_v8_bnfaccess	5*	1110*	
3*	4507*	219*	90*	22125*	36,420	3*	SHELLCODE_v88 inc v88 NOOP	4*	1361*	
3*	2905*	15043*	108*	80	33,763	TCP	WEB-MSC http directory traversal	5*	1063*	
3*	1543*	48*	28*	20432	30,490	TCP	DDOS shell client to handler	6*	401*	
3*	2815*	945*	69*	12832*	30,230	3*	SHELLCODE_v88 NOOP	5*	946*	
3*	9981*	12790*	217*	80	26,327	TCP	WEB-AS scripts access	5*	2250*	
3*	1063*	5915*	1717*	80	21,219	TCP	WEB-AS cmd exe access	3*	159*	
3*	201*	18704*	37*	80	20,363	TCP	WEB-MSC whistler HEAD with large diagram	4*	107*	
JAWA	76*	193*	211*	19,317	UDP	MSC Large UDP Packet	2*	29*		
3*	6203*	823*	70*	80	16,615	TCP	WEBFRONTPAGE_v8_rpc access	5*	1483*	
3*	127*	80	3497*	10192*	15,341	TCP	ATTACK RESPONSES 403 Forbidden	INSIDE	3*	
3*	849*	16*	26*	2*	13,979	TCP	DDOS mstream client to handler	5*	303*	
3*	3*	9258*	204*	80	13,887	TCP	WEB-AS multiple decode attempt	2*	2*	
2*	17*	25	1620*	5001*	13,602	TCP	POLICY SMTP relaying denied	2*	2*	
3*	3950*	7430*	81*	80	13,498	TCP	WEB-AS_v88 access	5*	1449*	
3*	305*	18*	546*	1742*	12,298	TCP	SCAN mmap TCP	3*	153*	
3*	197*	-1	212*	-1	11,016	3*	BAD TRAFFIC bad frag bits	2*	62*	
JANC	76*	76*	19*	161	10,027	UDP	SNMP request udp	UNKNOWN	U.S. DEPARTMENT OF TRANSPORTATION	
3*	563*	5343*	75*	80	9,500	TCP	WEB-CGI format access	3*	221*	

Alerts Aggregated
by Signature

Figure 10: Data View

Data View - Tuning Applied

Sorted by Hits

Alerts Aggregated by Organization

Site	Host IP	Port	Associated IP	Assoc Port	Hits	Prot	Signature	IP Category	Organization	Co
3*	412*	16405*	550*	47*	144,879	3*		343*	UNKNOWN	U.S. DEPARTMENT OF TRANSPORTATION
3*	2543*	9945*	950*	3713*	30,309	3*		328*		
3*	0*	0*	27*	777*	20,359	TCP		13*	UNKNOWN	THE NATIONAL OCEANIC AND ATMOSPHERIC ADMIN
3*	1017*	17352*	90*	270*	18,943	2*		69*		US
3*	3111*	7189*	1497*	109*	15,096	3*		74*	2*	AFRIC
3*	309*	3160*	100*	56*	12,130	TCP		43*	UNKNOWN	PAC BELL INTERNET SERVICES
3*	1233*	2672*	344*	16*	11,963	3*		60*	SUSPICIOUS	AOL
3*	2676*	4190*	147*	1094*	11,214	3*		84*	SUSPICIOUS	ATT NPT (REAL TIME MONITORING)
3*	1888*	4002*	476*	783*	10,059	3*		83*	SUSPICIOUS	RRE
3*	180*	864*	73*	700*	9,811	2*		56*		CERNET
2*	3*	3522*	12*	4*	9,482	TCP		29*	UNKNOWN	BOM INTERNATIONAL, INC.
3*	1289*	1417*	110*	821*	8,848	3*		72*	SUSPICIOUS	LEVEL 3 COMMUNICATIONS, INC.
3*	1214*	3231*	105*	229*	8,865	3*		68*	UNKNOWN	COMCAST CABLE COMMUNICATIONS, INC.
3*	160*	424*	56*	4324*	8,007	3*		42*	UNKNOWN	ABOVENET COMMUNICATIONS, INC.
3*	1145*	3190*	100*	56*	7,874	2*		71*	SUSPICIOUS	COX COMMUNICATIONS INC.
3*	88*	81*	35*	3755*	6,290	2*		21*	UNKNOWN	COSENT COMMUNICATIONS
3*	426*	431*	103*	1268*	6,076	2*		52*	UNKNOWN	CABLE 81 WIRELESS
3*	3*	2*	14*	20*	5,529	TCP		7*	UNKNOWN	SHOCKWAVE.COM
3*	674*	1241*	683*	149*	4,953	TCP		64*	UNKNOWN	QWEST COMMUNICATIONS
3*	326*	1032*	80*	270*	4,921	2*		54*	SUSPICIOUS	XO COMMUNICATIONS
3*	292*	4100*	4100*	4100*	4,815	3*		66*	UNKNOWN	VERIZON INC.

Figure 11: Data View – Tuning Applied

Data View - Organization Drilldown

Organization=U.S. DEPARTMENT OF TRANSPORTATION (IP Correlated Alerts) 412 rows from 144679 records

Site	Host IP	Port	Associated IP	Assoc port	Hits	Prot	Signature
3 *	192.168.254.240	15566 *	512 *	15 *	111,591	3 *	69 *
2 *	192.168.254.240	3893 *	41 *	7 *	18,170	2 *	69 *
IAMC	192.168.254.240	505 *	2 *	80	4,162	TCP	238 *
IAYVA	192.168.254.240	524	208.100.0.0	6 *	3,453	TCP	2 *
2 *	192.168.254.240	1993 *	2 *	80	2,851	TCP	8 *
2 *	192.168.254.240	2 *	2 *	9 *	980	TCP	8 *
IAMC	192.168.254.240	552 *	3 *	139	584	TCP	NETBIOS NT NULL session
2 *	192.168.254.240	523 *	17 *	3 *	538	2 *	21 *

Figure12: Data View – Organization Drilldown